PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-163469

(43)Date of publication of application : 20.06.1997

(51)Int.Cl. H04Q 9/00
E05B 65/20
// E05B 49/00

(21)Application number : 07-345398

(22)Date of filing : 11.12.1995

(71)Applicant : ALPHA CORP

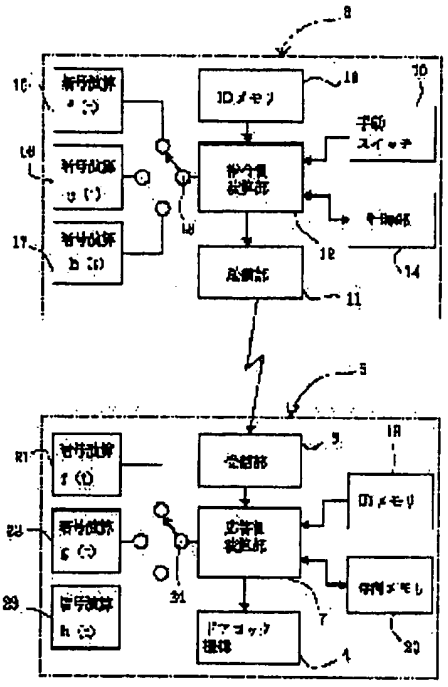
(72)Inventor : OGURO TAKESHI
YONEDA TSUTOMU

(54) DEVICE AND METHOD FOR REMOTE CONTROL

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the reliability and theft preventing property of entire device against an illegally imitated signal (key) by switching an enciphering system corresponding to information on change with the lapse of time.

SOLUTION: When the information showing the lapse of time as the information to be changed with the passage of time detected by a time measuring part 14 reaches a prescribed value, a command side arithmetic part 12 switches respective enciphering operation storage parts 15-16 storing enciphering operations as enciphering systems through a switching part 18. Since the system for enciphering an identification code is changed at every prescribed time, the imitated spare key is made ineffective and reliability and theft preventing property can be maintained and recovered.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－163469

(43)公開日　平成９年(1997)６月20日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｑ　9/00	３１１		Ｈ０４Ｑ　9/00	３１１Ｐ	
Ｅ０５Ｂ　65/20			Ｅ０５Ｂ　65/20		
// Ｅ０５Ｂ　49/00			49/00	Ｊ	

審査請求　未請求　請求項の数８　ＦＤ　（全 18 頁）

(21)出願番号　特願平7－345398

(22)出願日　平成７年(1995)12月11日

(71)出願人　000170598
株式会社アルファ
神奈川県横浜市金沢区福浦１丁目６番８号

(72)発明者　大黒　健
神奈川県横浜市金沢区福浦１－６－８　株式会社アルファテクニカルセンター内

(72)発明者　米田　勉
神奈川県横浜市金沢区福浦１－６－８　株式会社アルファテクニカルセンター内

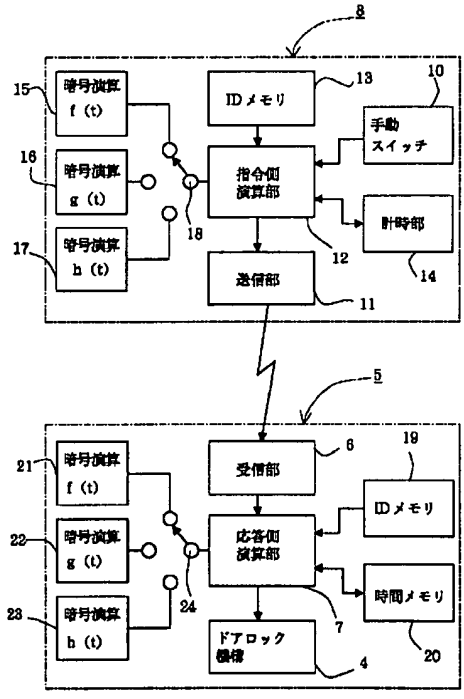
(74)代理人　弁理士　中村　猛

(54)【発明の名称】　遠隔操作装置及び遠隔操作方法

(57)【要約】

【課題】　出荷段階で固定的に定まる暗号化方式では、不正な模造信号（鍵）に対抗することができず、装置全体の信頼性が低下しうる。

【解決手段】　計時部１４が検出した経時変化情報としての経過時間情報が所定の値に達すると、指令側演算部１２は、切換部１８を介して、暗号化方式としての暗号演算を記憶した各暗号演算記憶部１５～１６を切り換える。所定時間毎に、識別コードを暗号化する方式が変更されるため、模造された合鍵を無力化して信頼性、防盗性を維持、回復することができる。



【特許請求の範囲】

【請求項１】　所定の識別コードを暗号化して送信する指令機と、この指令機からの識別コードを復号化して照合し、正規の識別コードであると判定したときには制御対象に制御信号を出力して所定の動作を行わせる応答機とを有する遠隔操作装置であって、

前記識別コードを暗号化するための暗号化方式を複数種類備え、経時的に変化する経時変化情報に基づいて前記複数種類の暗号化方式を切換使用することを特徴とする遠隔操作装置。

【請求項２】　所定の識別コードを暗号化して送信する指令機と、この指令機からの識別コードを復号化して照合し、正規の識別コードであると判定したときには制御対象に制御信号を出力して所定の動作を行わせる応答機とを有する遠隔操作装置であって、

前記指令機は、経時的に変化する経時変化情報を検出する経時変化情報検出手段と、予め登録された複数種類の暗号化方式の中から前記経時変化情報に基づいて特定の暗号化方式を選択する選択手段と、この選択された特定の暗号化方式に基づいて識別コードを暗号化信号に変換する暗号化信号生成手段と、この暗号化信号を前記応答機に向けて送信する送信手段とを備えて構成し、

前記応答機は、前記送信手段からの暗号化信号を受信する受信手段と、前記経時変化情報を検出する経時変化情報検出手段と、予め登録された前記複数種類の暗号化方式の中から前記経時変化情報に基づいて特定の暗号化方式を選択する選択手段と、この選択された特定の暗号化方式に基づいて前記暗号化信号を復号化する復号化手段と、この復号化された識別コードが正規の識別コードであるか否かを照合する照合手段と、この照合手段により正規の識別コードであると判定されたときには制御対象に制御信号を出力して所定の動作を行わせる制御信号出力手段とを備えて構成したことを特徴とする遠隔操作装置。

【請求項３】　指令機と応答機との間で信号波を送受信することにより指令機の有する識別コードが正規の識別コードであると応答機が判定したときに、該応答機が制御対象に制御信号を出力して所定の動作を行わせる遠隔操作装置であって、

前記指令機は、第１の識別コードを前記応答機に向けて送信する第１の送信手段と、経時的に変化する経時変化情報を検出する経時変化情報検出手段と、予め登録された複数種類の暗号化方式の中から前記経時変化情報に基づいて特定の暗号化方式を選択する選択手段と、この選択された特定の暗号化方式に基づいて識別コードを暗号化信号に変換する暗号化信号生成手段と、前記応答機からの応答信号を受信したときに前記暗号化信号を前記応答機に向けて送信する第２の送信手段とを備えて構成し、

前記応答機は、前記第１の送信手段からの第１の識別コードを受信する第１の受信手段と、この受信した第１の識別コードが正規の識別コードであるか否かを判定する第１の照合手段と、この第１の照合手段が正規の識別コードであると判定したときには前記指令機に向けて応答信号を送信する応答信号送信手段と、この応答信号により前記第２の送信手段から送信された暗号化信号を受信する第２の受信手段と、前記経時変化情報を検出する経時変化情報検出手段と、予め登録された前記複数種類の暗号化方式の中から前記経時変化情報に基づいて特定の暗号化方式を選択する選択手段と、この選択された特定の暗号化方式に基づいて前記暗号化信号を復号化する復号化手段と、この復号化された識別コードが正規の識別コードであるか否かを照合する第２の照合手段と、この第２の照合手段により正規の識別コードであると判定されたときには制御対象に制御信号を出力して所定の動作を行わせる制御信号出力手段とを備えて構成したことを特徴とする遠隔操作装置。

【請求項４】　前記選択手段は予め登録された複数種類の暗号化方式を所定の切換順序に従って選択し、この所定の切換順序の進行状況を監視する切換順序監視手段を設けたことを特徴とする請求項２又は請求項３のいずれかに記載の遠隔操作装置。

【請求項５】　前記指令機又は前記応答機のいずれか一方の経時変化情報検出手段で検出した経時変化情報を他方の経時変化情報検出手段に報知し、該他方の経時変化情報検出手段は、この報知された経時変化情報に基づいて間接的に経時変化情報を検出することを特徴とする請求項２～４のいずれかに記載の遠隔操作装置。

【請求項６】　前記経時変化情報として、時間情報又は前記指令機の操作回数の少なくともいずれかを用いることを特徴とする請求項１～５のいずれかに記載の遠隔操作装置。

【請求項７】　前記指令機には強制切換信号生成手段を設け、該強制切換信号生成手段によって生成された切換信号により、前記複数種類の暗号化方式を切り換えることを特徴とする請求項１～６のいずれかに記載の遠隔操作装置。

【請求項８】　指令機と応答機とを備え、所定の識別コードを暗号化して応答機に送信する送信ステップと、この暗号化された識別コードを復号化する復号化ステップと、この復号化された識別コードを照合して正規の識別コードであるか否かを判定する照合ステップと、正規の識別コードであると判定したときには制御対象に制御信号を出力して所定の動作を行わせる制御信号出力ステップとを有する遠隔操作方法であって、

経時的に変化する経時変化情報を検出する経時変化情報検出ステップと、

この経時変化情報に基づいて予め登録された複数種類の暗号化方式を切換選択する切換選択ステップとを設けたことを特徴とする遠隔操作方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば自動車用ドアロック等に用いて好適な遠隔操作装置及び遠隔操作方法に関し、特に、複数種類の暗号化方式を備えた遠隔操作装置及び遠隔操作方法に関する。

【0002】

【従来の技術】一般に、遠隔操作装置及び遠隔操作方法としては、例えばテレビジョン受像機やエアコンディショナー等の遠隔操作の他に、自動車のドアロックを遠隔で施錠又は解錠するキーレスシステム等が知られている。ここで、例えば自動車用ドアロック等の如く防盗・性、防犯性が要求される場合は、正当な所有者が有するリモートキーと車体側のロック装置とを一対一で対応せしめ、これにより、他人のリモートキーによる不正な解錠を阻止して窃盗等を未然に防止している。即ち、各リモートキーにそれぞれ記憶された固有の識別コードと車体側のロック装置が記憶した識別コードとを照合し、両コードが一致するときにのみドアロックを解除する。

【0003】また、識別コードをそのまま送信すると、第三者が容易に解読して模造キーを作成しうるので、以下に述べる如く、乱数等によって識別コードを暗号化して送信する技術が種々提案されている。

【0004】即ち、第2の従来技術として、例えば特開平6－339036号公報等に記載のものでは、ファクシミリ装置で送信する平文データを秘密鍵で暗号化し、相手側のファクシミリ装置で暗号データを解読するようになっている。ここで、この第2の従来技術では、第三者による解読を防止するため、暗号化に用いる秘密鍵を年月日や時刻等の暦データによって所定期間毎に変更している。従って、この第2の従来技術によれば、送信側のファクシミリ装置と受信側のファクシミリ装置との時刻が許容誤差内で同期している限り、第三者による解読を困難にしつつ受信側ファクシミリ装置で容易に解読することが可能である。

【0005】さらに、第3の従来技術としては、例えば特開平1－192970号公報等に記載の如く、制御対象の一例としてのロック機構を作動させる識別コード（鍵）を第1の識別コードと第2の識別コードとに分割し、第1の識別コードの照合完了後に車体側から返信された乱数に基づいて第2の識別コードを送信するようにしたものが知られている。従って、この第3の従来技術によるものでは、リモートキー側と車体のロック装置側との交信によって解錠又は施錠を行うため、一層防盗性を高めることができる。

【0006】

【発明が解決しようとする課題】ところで、上述した各従来技術によるものでは、暗号化に用いる秘密鍵を暦データに基づいて変更したり、識別コードを分割したりして、第三者による不正行為を未然に防止せんとしているが、いずれの場合も、暗号化の方式（暗号化手法又は暗号化パターン）は、製品の出荷段階で定められ、一度設定された暗号化方式は、その製品寿命が尽きるまで変化することがない。従って、固定的に設定された暗号化方式が、やがて第三者によって解読されてしまうおそれがあり、解読された場合には、識別コードの異なる他の製品についても合鍵が作成されてしまい、装置全体の信頼性が低下する可能性がある。

【0007】即ち、識別コードを暗号化する基本的な方式としては、例えば転置、換字等の複数の方式が知られているが、従来技術によるものでは、これら複数種類の暗号化方式のうち、いずれか一種類の暗号化方式を設計段階ないし出荷段階で固定的に設定するため、設定された暗号化方式が解読されてしまうと、たとえ製品毎に固有の識別コードが付与されていても、比較的容易に合鍵を模造することが可能となる。特に、自動車のように比較的高額で窃盗等の対象になり易い特質を備えた製品では、合鍵の模造を図る者が後を断たず、防盗性の低下という脅威にさらされている。

【0008】本発明は、かかる従来技術の問題に鑑みてなされたもので、その目的は、信頼性、防盗性を向上できるようにした遠隔操作装置及び遠隔操作方法を提供することにある。

【0009】

【課題を解決するための手段】そこで、本発明は、例えば転置、換字等の如く、複数の暗号化方式を予め設定しておき、経時的に変化する情報に基づいて暗号化方式を切換使用することにより、ある時点で第三者により模造、複製された合鍵を暗号化方式の自動切換によって無力化し、これにより、遠隔操作装置及び遠隔操作方法の信頼性、防盗性を高いレベルに維持、回復できるようにした。

【0010】即ち、本発明に係る遠隔操作装置は、所定の識別コードを暗号化して送信する指令機と、この指令機からの識別コードを復号化して照合し、正規の識別コードであると判定したときには制御対象に制御信号を出力して所定の動作を行わせる応答機とを有する遠隔操作装置であって、前記識別コードを暗号化するための暗号化方式を複数種類備え、経時的に変化する経時変化情報に基づいて前記複数種類の暗号化方式を切換使用することを特徴としている。

【0011】この請求項1の構成により、時間の経過と共に変化する経時変化情報によって暗号化方式が切り換えられるため、ある時点で指令機が模造された場合、即ち、ある時点で採用されている一の暗号化方式に従った暗号化信号を送信できる偽指令機が製造された場合でも、経時変化情報に基づいて他の暗号化方式に切り換えられた時点で、この偽指令機は無力化し、その後使用不能となる。従って、不正な模造信号の生成を阻止できずとも、経時変化情報の性質で定まる所定サイクル毎に、

遠隔操作装置の信頼性、防盗性を回復することができる。

【００１２】ここで、「経時的に変化する経時変化情報」とは、時間の進行に伴って値が順次変化（増大変化又は減少変化の両方を含み、アナログ的変化、デジタル的変化のいずれでもよい）する情報を意味しており、具体的には、例えば年月日、時分秒等の時間、指令機の操作回数（又は応答機の作動回数）、制御対象の動作回数等をいう。また、「複数種類の暗号化方式」とは、例えば転置、換字の如く、暗号化の手法が異なる方式を２以上備えていることを意味する。

【００１３】また、請求項２に係るものでは、指令機と応答機の双方が、それぞれ経時変化情報を検出して、複数種類の暗号化方式の中から特定の暗号化方式を選択するため、指令機及び応答機は、経時変化情報に基づいて、予め登録された複数の暗号化方式の中から常に同一の暗号化方式を選択するように切り換える。従って、正規の指令機と応答機との間では指令が正確に伝送されて制御対象に所望の動作を行わせることができる上に、模造された指令機は、やがて行われる暗号化方法の切換選択によって無力化するため、不正な遠隔操作が継続的に行われることを未然に防止することができる。

【００１４】請求項３に係るものでは、応答機の作動に必要な識別コードを第１の識別コードと第２の識別コードとに分割し、かつ、第１の識別コードの照合終了後に、経時変化情報に基づいて暗号化された第２の識別コードを送信する構成のため、上記請求項２よりも防盗性を高めることができる。

【００１５】請求項４に係るものでは、選択手段は予め登録された複数種類の暗号化方式を所定の切換順序に従って選択し、この所定の切換順序の進行状況を監視する切換順序監視手段を設けたため、万が一、正規の指令機が記憶する複数種類の暗号化方式を全て複製した模造指令機が製造された場合であっても、その切換順序が異なれば、応答機による制御対象を動作させることができず、より一層防盗性、信頼性を高めることができる。

【００１６】請求項５に係るものでは、指令機又は応答機のいずれか一方の経時変化情報検出手段で検出した経時変化情報を他方の経時変化情報検出手段に報知し、該他方の経時変化情報検出手段は、この報知された経時変化情報に基づいて間接的に経時変化情報を検出する構成のため、実際に経時変化情報を検出するのは指令機又は応答機の経時変化情報検出手段のうちいずれか一方のみで足り、他方は、その検出された値を自己の検出値として間接的に検出することになる。従って、全体構造を簡素化しつつ、指令機と応答機との間で経時変化情報にずれが生じるのを確実に防止することができる。

【００１７】請求項６に係るものでは、前記経時変化情報として、時間情報又は前記指令機の操作回数の少なくともいずれかを用いるため、複数種類の暗号化方式を、時間情報又は指令機の操作回数によって容易に切り換えることができる。

【００１８】請求項７に係るものでは、前記指令機には強制切換信号生成手段を設け、該強制切換信号生成手段によって生成された切換信号により、前記複数種類の暗号化方式を切り換えるため、経時変化情報による暗号化方式の切換とは別に、所望の時点で暗号化方式を強制的に切り換えることができ、より一層防盗性を高めることができる。

【００１９】請求項８に係る遠隔操作方法では、前記請求項１と同様に、経時変化情報によって暗号化方式を自動的に切換選択することができ、万が一、ある時点で指令機が偽造された場合でも、その偽造指令機を所定サイクル毎に無力化することができる。

【００２０】

【発明の実施の形態】以下、本発明の実施の形態を、図１～図１３に基づき、遠隔操作装置及び遠隔操作方法としての自動車用ドアロックシステムに適用した場合を例に挙げて説明する。

【００２１】まず、図１～図４は、本発明の第１の実施の形態に係る遠隔操作装置を自動車用ドアロックシステムに採用した場合の全体構成図であって、自動車１の前後左右に配設されたドア２のアウトサイドハンドル２Ａ又は該ハンドル２Ａの近傍には、図示せぬキーを挿入するためのキーシリンダ３が設けられ、このキーシリンダ３は、「制御対象」としてのドアロック機構４に接続されている。このドアロック機構４は、キーシリンダ３に正規のキーが挿入された場合、後述する指令機８による所定の識別コードが送信された場合等に、図示せぬ電磁ソレノイド等のアクチュエータを駆動してドア２を施錠又は解錠するものである。なお、このドアロック機構４には、例えばマイクロスイッチ、近接スイッチ等からなり、施錠又は解錠の状態を検出する状態検出スイッチ（図示せず）が設けられ、この状態検出スイッチは後述の応答側演算部７に接続されている。

【００２２】ドア２には、指令機８によってドアロック機構４を制御する応答機５が設けられ、この応答機５は、受信部６で受信した暗号化信号を応答側演算部７で解読して照合し、正規の識別コードであると判定した場合に、ドアロック機構４に制御信号を出力して、「所定の動作」としての施錠又は解錠を行わせるようになっている。ここで、受信部６としては、電波信号を受信する場合は例えばフェライトバーアンテナ、スーパーヘテロダイン受信機等を用いればよく、光信号を受信する場合には例えばフォトトランジスタ等を用いればよく、受信部６の取付位置はドア２に限定されない。

【００２３】自動車１の正当な所有者が所持するリモートキーとしての指令機８は、略カード状のケーシング９と、このケーシング９に設けられた手動スイッチ１０と、この手動スイッチ１０の操作によって暗号化信号を

外部に送信するフェライトバーアンテナ等からなる送信部１１と、後述の指令側演算部１２等とを備えて構成されている。

【００２４】次に、上述した応答機５及び指令機８の具体的構造について図２のブロック図を参照しつつ説明する。

【００２５】まず、指令機８は、ＣＰＵ等からなり、後述の暗号化演算に基づいて識別コードを暗号化するための指令側演算部１２と、この暗号化信号を応答機５側に向けて送信するための送信部１１と、固有の識別コード（以下「ＩＤ」と示す）を記憶したＲＯＭ等からなるＩＤメモリ１３と、経時変化情報としての時間情報を生成するためのクロック等からなる計時部１４と、それぞれ異なる複数の「暗号化方式」としての暗号演算ｆ(ｔ)，ｇ(ｔ)，ｈ(ｔ)を記憶したＲＯＭ等からなる例えば３個の暗号演算記憶部１５，１６，１７（図中「暗号演算」と略記）と、これら各暗号演算記憶部１５，１６，１７を選択的に切り換えるための切換部１８とから構成されている。

【００２６】ここで、計時部１４は、クロックと、例えば１０ｍｓ毎にカウントアップするＮ（Ｎ＞８）桁の１６進カウンタ（C_N，C_{N-1}，…C_1：各桁は０～Ｆ）とを有している。そして、この計時部１４は、予め設定された所定の桁がカウントアップすると、暗号演算の切換時期が到来したことを報知すべくカウントアップ信号を指令側演算部１２に出力するものである（１０ｍｓ毎に計時した場合、１６進カウンタの８桁目がカウントアップする周期は、約３１日となる）。

【００２７】なお、カウントアップ信号を出力する所定の桁は、出荷時等で固定的に設定してもよいし、あるいは指令側演算部１２から適宜設定変更できるようにしてもよい。さらに、暗号演算の切換時期は防盗性等を考慮して定められるもので、約３１日に限らず、例えば１時間、１日、１週間毎に切り換えてもよい。即ち、例えば１００ｍｓ毎に暗号演算を切り換える場合は、指令信号を模造した直後に、暗号演算が循環的に切り換わって、応答機５が模造信号に応答してしまう確率が高くなるため、切換周期を短くすれば防盗性が向上する訳ではない。一方、例えば３カ月毎に暗号演算を切り換える場合は、模造信号の有効期間が長くなるため、その間に不正行為が行われる可能性が上昇する。従って、この切換周期は、模造信号の作成時期と不正行為の実行時期とのずれ等を考慮して定められる。このため、例えば、休日の使用が多いマイカーの場合は１カ月程度に、略毎日使用する営業車の場合は１週間毎に設定する等、その車両の特質に応じて設定する構成とすればよい。

【００２８】また、計時部１４をクロックで構成し、指令側演算部１２で時間情報をカウントする構成でもよく、カウント周期も１０ｍｓに限定されない。さらに、時間情報を計時するカウンタは、積算カウンタでもよいし、あるいは設定値に達する毎にリセットされるプリセットカウンタとして構成してもよい。

【００２９】切換部１８は、指令側演算部１２からの切換信号に応じて、所定の順序で各暗号演算記憶部１５，１６，１７を順番に切換選択するもので、計時部１４の時間値が所定値に達する度に、例えば第１の暗号演算記憶部１５から第２の暗号演算記憶部１６へ、該第２の暗号演算記憶部１６から第３の暗号演算記憶部１７へ、第３の暗号演算記憶部１７から第１の暗号演算記憶部１５へと循環的に切り換えるものである（１５→１６→１７→１５…）。但し、切換順序は、暗号演算記憶部の符号順に限らず、その逆（１７→１６→１５→１７…）でもよいし、あるいは、任意の順序（例えば１５→１７→１６→１５…）に設定してもよい。

【００３０】ここで、各暗号演算記憶部１５～１７の具体的暗号生成手法について例示すると、第１の暗号演算記憶部１５が記憶する暗号演算ｆ(ｔ)は「換字」を行い、第２の暗号演算記憶部１６が記憶する暗号演算ｇ(ｔ)は「転置」を行い、第３の暗号演算記憶部１７が記憶する暗号演算ｈ(ｔ)は「換字」処理後に「転置」を行うように構成してもよい。

【００３１】即ち、例えばＩＤコードを「I_1，I_2，I_3，I_4，I_5，I_6，I_7」の１６進数の７桁とし、計時部１４では８桁目のC_8がカウントアップする度にカウントアップ信号を出力するものとすると、前記第１の暗号演算ｆ(ｔ)は、下記数１に示す如く、ＩＤコードの各桁と時間情報の各桁の１６進カウンタ値との排他的論理和（ＸＯＲ）をとって、A_7，A_6，…A_1の新たなコードに変換するようになっている。

【００３２】

【数１】$I_7(XOR)C_7$，$I_6(XOR)C_6$，$I_5(XOR)C_5$…$I_1(XOR)C_1 \rightarrow A_7$，$A_6$，…$A_1$

そして、上記数１の如く換字した後、指令側演算部１２は、下記数２に示す如く、時間情報のカウンタ値に換字によって暗号化された信号を付加して送信部１１から応答機５に向けて送信するようになっている。

【００３３】

【数２】C_N，C_{N-1}，…C_1，A_7，A_6，…A_1

また、転置を行う第２の暗号演算ｇ(ｔ)は、下記表１に示す如く、計時カウンタの最下位の桁C_1の値（０～Ｆ）毎に用意された転置パターンP_0～P_Fによって、ＩＤコードの各データI_7～I_1を並べ替えるものである。従って、並替のパターンP_0～P_Fは１０ｍｓ毎に切り換えられている。

【００３４】

【表１】

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_A	P_B	P_C	P_D	P_E	P_F

そして、指令側演算部１２は、下記数３に示す如く、この並べ替えられたＩＤコードに時間情報のカウンタ値を付加し、これを送信部１１から応答機５に向けて送信するようになっている。

【００３５】

【数３】C_N，C_{N-1}，…C_1，I_2，I_4，I_7，I_3，I_6，I_1，I_5

また、複合演算を行う第３の暗号演算ｈ(ｔ)は、まず最初に前記第１の暗号演算ｆ(ｔ)と同様の換字処理を行ってＩＤコードをA_7～A_1に変換した後、次に、この換字化コードA_7～A_1を前記第２の暗号演算ｇ(ｔ)と同様に、最下位のカウンタ値C_1で定まる所定の並替パターンP_0～P_Fに従って転置するようになっている。

【００３６】なお、本実施の形態では、説明及び理解の便宜上、暗号演算の種類を３種類にしているが、暗号演算の種類数は、防盗性、信頼性の要求レベル、製造コスト等を総合的に考慮して定められるものであるため、３種類に限定されない。例えば好ましくは、３種類～１０種類の範囲で、より好ましくは、５種類程度に暗号演算の種類を設定すればよい。これらの範囲に設定すれば、指令機８の偽造コストを大幅に上昇させることができる上に、暗号演算を順次切り換えて試すのに要する時間が長くなって不正行為が露見する機会も増大するため、不正行為の抑止効果を得ることができる。但し、暗号演算の種類を２種類にしたものも本発明の範囲に含まれる。さらに、暗号化方式の一例として、換字、転置、換字及び転置の３種類を挙げたが、これに限らず、他の暗号化方式を採用してもよい。

【００３７】一方、自動車１側に設けられた応答機５は、指令機８からの暗号化信号を受信する受信部６と、ＣＰＵ等からなる応答側演算部７と、前記指令機８側のＩＤコードに対応するＩＤコード（一般に両コードは同一である）を記憶したＲＯＭ等からなるＩＤメモリ１９と、指令機８の計時部１４が計測したカウンタ値を更新記憶する時間メモリ２０と、前記各暗号演算記憶部１５，１６，１７と同一の暗号演算ｆ(ｔ)，ｇ(ｔ)，ｈ(ｔ)をそれぞれ記憶した暗号演算記憶部２１，２２，２３と、これら各暗号演算記憶部２１～２３を時間メモリ２０の時間情報に応じて切り換える切換部２４とから構成され、応答側演算部７はドアロック機構４に接続されている。そして、応答機５は、指令機５から受信した信号中の時間情報のカウンタ値に従って各暗号演算記憶部２１～２３を選択的に切り換え、これによりＩＤコードを照合してドアロック機構４の動作を制御するものである。

【００３８】次に、図３及び図４のフローチャートを参照しつつ本実施の形態の作用について説明する。

【００３９】まず、図３は、指令機８による送信処理を示すフローチャートであって、計時部１４は、ステップ（図中では、ステップを「Ｓ」と略記）１で、図示せぬ電池のセット時からの経過時間を計測しており、次のステップ２では、手動スイッチ１０の状態を読込んで、該手動スイッチ５が操作されたか否かを監視する。このステップ２で「ＹＥＳ」と判定したときは、操作者が施錠又は解錠を希望する場合のため、ステップ３に移り、このステップ３では、ＩＤメモリ１３からＩＤコードを読込む。

【００４０】次に、ステップ４では、前記ステップ１で計時している現在の時間情報（カウンタ値）が所定時間（例えば３１日）を越えているか否か、即ち８桁目のC_8がカウントアップしたか否かを計時部１４からのカウントアップ信号の有無で判定する。但し、上述した通り、計時部１４からカウントアップ信号を出力せず、指令側演算部１２内でカウンタ値が所定値に達したか否かを判定してもよい。

【００４１】このステップ４で「ＮＯ」と判定したときは、まだ所定時間が経過せず、暗号化方式、即ち暗号演算を切り換える必要がない場合のため、ステップ５では、前回更新記憶された暗号演算（ｆ(ｔ)，ｇ(ｔ)，ｈ(ｔ)のいずれか一つ）を切換部１８により選択する。なお、初期状態では、初期値として、例えば第１の暗号演算記憶部１５の暗号演算ｆ(ｔ)が設定されている。一方、前記ステップ４で「ＹＥＳ」と判定したときは、前回の暗号演算切換時からの経過時間が所定時間を越えている場合のため、ステップ６に移り、このステップ６では、切換部１７によって、次の暗号演算記憶部（例えば第２の暗号演算記憶部１６）を選択し、次のステップ７では、この新たに選択された暗号演算（ｇ(ｔ)）を更新記憶する。

【００４２】そして、ステップ８では、前記ステップ５又はステップ７で選択された暗号演算に基づいてＩＤコードを暗号化し、次のステップ９では、この暗号化されたＩＤコードに時間情報（カウンタ値）を付加して送信部１１から応答機５に向けて送信する。

【００４３】次に、図４は、応答機５側の受信処理を示すフローチャートであって、まず、ステップ１１では、受信部６を監視して指令機８からの指令信号を受信したか否かを判定する。そして、このステップ１１で「ＹＥＳ」と判定したときは、受信部６が指令機８からの信号を受信した場合のため、ステップ１２では、この信号中に含まれる時間情報を取り出し、この現在の受信時の時間情報が時間メモリ２０内に記憶された前回受信時の時

間情報よりも進んでいるか否かを判定する。このステップ１２で「ＮＯ」と判定したときは、時間情報が前回受信時よりも進んでいない場合、即ち、偽造された信号を受信した場合か、又は他の同様の指令機からの信号が混信している場合等のため、暗号化されたＩＤコードを照合する必要もなく、この受信した信号を無視してステップ１１に戻る。一方、前記ステップ１２で「ＹＥＳ」と判定したときは、前記ステップ１１で受信した時間情報が前回受信時の時間情報よりも進んでいる正常な場合であるため、ステップ１３に移って、所定時間が経過したか否かを判定する。

【００４４】このステップ１３で「ＮＯ」と判定したときは、時間情報が所定時間を経過していない場合のため、ステップ１４に移って、前回更新記憶された暗号演算を選択する。一方、前記ステップ１３で「ＹＥＳ」と判定したときは、受信した信号中の時間情報が所定時間を越えている場合のため、ステップ１５に移り、このステップ１５では、所定の順序に従って切換部２４により暗号演算を切り換え、次のステップ１６では、この新たに選択した暗号演算を更新記憶する。

【００４５】そして、ステップ１７では、前記ステップ１４又はステップ１６で選択された暗号演算に基づいて暗号化されたＩＤコードを解読（復号化）し、ステップ１８では、ＩＤメモリ１９から応答側のＩＤコードを読込み、ステップ１９では、これら指令側のＩＤコードと応答側のＩＤコードとを照合して、両コードが一致するか否かを判定する。

【００４６】このステップ１９で「ＮＯ」と判定したときは、偽造された信号である場合、又は他の同様の指令機からの信号を偶然解読できた場合等であるため、以後の処理を行わずに前記ステップ１１に戻る。一方、前記ステップ１９で「ＹＥＳ」と判定したときは、指令信号中の暗号化ＩＤコードと応答機５に設定されたＩＤコードとが一致する場合のため、ステップ２０では、ドアロック機構４に制御信号を出力してドア２を施錠又は解錠せしめ、ステップ２１では、今回受信した指令信号中の時間情報を時間メモリ２０に更新記憶する。ここで、前記ステップ１９では、両ＩＤコードの一致、不一致を判定するものとして述べたが、これに限らず、例えば両ＩＤコードが補数の関係にある場合等の如く、指令機８側のＩＤコードと応答機５側のＩＤコードとに所定の対応関係を設定しておき、正常な対応関係が成立しているか否かを判定してもよい。

【００４７】このように構成される本実施の形態によれば、以下の効果を奏する。

【００４８】第１に、ＩＤコードを暗号化するための暗号演算をｆ(ｔ)，ｇ(ｔ)，ｈ(ｔ)の３種類備え、経時的に変化する時間情報に基づいて前記３種類の暗号演算を切換使用する構成のため、施錠又は解錠の仕組みを所定時間毎に変化させることができ、指令機８の指令信号の偽造を困難化できると共に、万が一、指令信号が偽造された場合でも、この偽造信号を所定時間後に無力化することができるため、防盗性、信頼性を常に高いレベルで保持、回復することができる。

【００４９】第２に、時間情報に基づいて暗号演算を切り換える構成のため、絶えず変化する時間情報に基づいて暗号演算を連続的に切り換えることができ、指令機８の操作に拘わらず、システムの信頼性等を容易に維持することができる。

【００５０】第３に、経時変化情報としての時間情報を指令機８の計時部８でのみ計測し、応答機５側では、計時部８が計測した時間情報を時間メモリ２０に記憶して用いる構成のため、全体構造を簡素化して製造コストを低減できる上に、指令機８側と応答機５側とで「時間ずれ」が生じるのを確実に回避して、安定した施錠又は解錠動作を得ることができる。即ち、従来技術の如く、両方にタイマを設ける場合は、このタイマの分だけ部品コスト、組付コストが増大するばかりか、両者の間の「時間ずれ」を完全に回避することができないため、何らかの対策を要し、制御構造も複雑化する。これに対し、本実施の形態では、応答機５で時間情報を検出せず、指令機８側で検出した時間情報に従うため、全体構造が簡素化すると共に信頼性が高まる。

【００５１】第４に、応答機５側では、指令機８から受信した信号中の時間情報が前回受信時の時間情報よりも進んでいるか否かを判定し、現在の時間情報の方が進んでいる場合にのみ、暗号化されたＩＤコードを復号化する構成のため、指令信号の偽造を一層困難にすることができる上に、混信や偽造信号の場合の無駄な解読を防止してエネルギ消費を節約することができる。

【００５２】第５に、３種類の暗号演算ｆ(ｔ)，ｇ(ｔ)，ｈ(ｔ)を所定の順序で切り換えて循環的に使用する構成のため、各暗号演算部１５～１７，２１～２３のメモリ消費量を節約することができる。即ち、例えば、自動車１の最大耐用年数を２０年に設定し、１カ月毎に暗号演算を切り換えるものとして、２４０種類の暗号演算を予め登録しておき、一度使用した暗号演算は再使用しないように構成することも可能であるが、この場合には、多量のメモリを消費する。しかし、本実施の形態では、暗号演算を循環的に切換使用するため、最小限のメモリ消費量にすることができる。但し、上述した製品最大寿命にわたって新たな暗号演算を使用する構成も本発明の範囲に含まれる。

【００５３】次に、図５～図７を参照しつつ本発明の第２の実施の形態を説明する。なお、以下の各実施の形態では、上述した第１の実施の形態と同一の構成要素に同一の符号を付し、その説明を省略するものとする。本実施の形態の特徴は、経時的に変化する情報として、指令機の操作回数を用いた点にある。

【００５４】即ち、図５は、本実施の形態に係る遠隔操

作装置の構成を示すブロック図であって、応答機３１は、前記実施の形態で述べた応答機５と同様に、受信部６、応答側演算部７、ＩＤメモリ１９、各暗号演算記憶部２１～２３、切換部２４を備え、応答側演算部７はドアロック機構４に接続されている。しかし、この応答機３１には、前記時間メモリ２０に代えて、後述の指令機３３から送信されたカウンタ情報を記憶するカウンタメモリ３２が配設されている点で、前記実施の形態とは異なる。

【００５５】一方、指令機３３も、前記実施の形態で述べた指令機８と同様に、ケーシング９、手動スイッチ１０、送信部１１、指令側演算部１２、ＩＤメモリ１３、各暗号演算記憶部１５～１７、切換部１８を備えて構成されている。しかし、この指令機３３には、前記計時部１４に代えて、手動スイッチ１０の操作回数（指令機３３の送信回数）を計数するカウンタ３４が設けられている点で、前記実施の形態とは異なる。即ち、このカウンタ３４は、手動スイッチ１０が操作される毎に累進するもので、これにより送信回数を記憶しておくものである。

【００５６】次に、図６及び図７を参照しつつ本実施の形態の作用を説明する。まず、図６は、指令機３３側の送信処理を示し、時間情報に代えて操作回数（送信回数）を用いる点を除き、図３と共に述べた送信処理と同様の処理を行う。

【００５７】即ち、ステップ３１では、手動スイッチ１０が操作されたか否かを監視し、手動スイッチ１０が操作された場合は「ＹＥＳ」と判定して、ステップ３２でカウンタ３４を累進させる。次に、ステップ３３では、ＩＤメモリ１３からＩＤコードを読込んでおき、ステップ３４では、前記ステップ３２で累進させたカウンタ３４のカウント値（カウンタ情報）が、予め設定された所定の回数に達したか否かを判定する。このステップ３４で「ＮＯ」と判定したときには、指令機３３の操作回数が所定の回数に達していない場合のため、ステップ３５に移って、前回更新された暗号演算を選択する。ここで、前記所定の回数は、第１の実施の形態で述べた時間情報の設定値と同様に、自動車１の使用頻度、防盗性等を考慮して定められる。一方、前記ステップ３４で「ＹＥＳ」と判定したときは、指令機３３の操作回数が所定の回数に達した場合のため、ステップ３６に移って、切換部１８により暗号演算を切り換え、ステップ３７では、この切り換えられた新たな暗号演算を更新記憶する。

【００５８】そして、ステップ３８では、前記ステップ３５又はステップ３６で選択された暗号演算に基づいてＩＤコードを暗号化し、ステップ３９では、この暗号化されたＩＤコードにカウンタ情報を付加して送信部１１から送信する。

【００５９】次に、図７は、応答機３１側の受信処理を示し、この受信処理も、時間情報の代わりに指令機３３の操作回数を用いる点を除き、図４と共に上述した応答処理と同様の処理を行うものである。

【００６０】まず、ステップ４１では、指令機３３からの指令信号を受信部６が受信したか否かを監視しており、受信した場合には「ＹＥＳ」と判定して、ステップ４２に移り、このステップ４２では、指令信号中のカウンタ情報（操作回数）がカウンタメモリ３２に記憶された前回受信時のカウンタ情報よりも大きいか否かを判定する。このステップ４２で「ＮＯ」と判定したときは、カウンタ情報が前回受信時よりも進んでいない場合、即ち、模造された指令信号又は他の指令機からの信号を受信した場合等であり、その後の処理を実行する意味がないため、今回の受信を無視して前記ステップ４１に戻る。

【００６１】一方、前記ステップ４２で「ＹＥＳ」と判定したときは、カウンタ情報が前回受信時よりも大きい正常な場合のため、ステップ４３に移り、このステップ４３では、カウンタ情報が所定の回数に達したか否かを判定する。そして、このステップ４３で「ＮＯ」と判定したときは、ステップ４４で、前回選択された暗号演算をそのまま引続き使用し、前記ステップ４３で「ＹＥＳ」と判定したときは、ステップ４５で暗号演算を切り換え、ステップ４６で、この新たな暗号演算を更新記憶する。

【００６２】次に、ステップ４７では、前記ステップ４４又はステップ４５で選択された暗号演算に基づいて指令信号中の暗号化ＩＤコードを復号化する。そして、ステップ４８では、ＩＤメモリ１９からＩＤコードを読込み、ステップ４９では、この指令側ＩＤコードと応答側ＩＤコードとが一致するか否かを判定し、両者が一致した場合には「ＹＥＳ」と判定して、ステップ５０に移る。ステップ５０では、ドアロック機構４に施錠又は解錠を要求する制御信号を出力し、ステップ５１では、カウンタメモリ３２のカウンタ情報を更新する。

【００６３】このように構成される本実施の形態でも、上述した第１の実施の形態と略同様の効果を得ることができる。これに加えて、本実施例では、経時変化情報として、指令機３３の操作回数を用いる構成のため、切換時期の固定化を防止することができ、防盗性を向上することができる。即ち、時間情報を用いる場合は、例えば３１日毎の如く、規則的に暗号演算が切り換えられるため、この切換周期が万が一知られた場合には、防盗性が低下する可能性があるが、操作回数によって暗号演算を切り換える場合は、切換時期が変則的になるため、模造信号の有効期間を推測するのが困難となり、防盗性が高まる。なお、時間情報と操作回数の双方を切換時期検出用パラメータ（経時変化情報）として使用し、いずれか一方が所定値に達したときに暗号演算を切り換える構成としてもよい。

【００６４】また、操作回数に基づいて暗号演算を切り換える構成のため、計時手段としてのタイマを設ける必要がなく、電力消費量を低減できると共に、全体構造を簡素化して製造コストも低減することができる。即ち、時間情報に基づいて暗号演算を切り換える場合は、交信用のタイマのほかに、時間情報を計時するためのタイマを別途設ける必要があるため、電力消費量が増大し、構造が複雑化する。リモートキーとして用いられる指令機３３のような携帯型の機器では、特に、電池寿命の長期化が要求されるため、電力消費量の低減は重要な効果となる。

【００６５】次に、図８～図１０に基づいて本発明の第３の実施の形態を説明する。本実施の形態では、前記第２の実施の形態と同一の構成要素に同一の符号を付し、その説明を省略するものとする。本実施の形態の特徴は、指令機側の電池交換時に強制的に暗号演算の切換信号を出力するようにした点と、指令機側で選択された暗号演算に応答機側が従うように構成した点とにある。

【００６６】即ち、図８は、本実施の形態に係る遠隔操作装置のブロック図であって、応答機４１は、前記第２の実施の形態で述べた応答機３１と同様に、受信部６、ＩＤメモリ１９、各暗号演算記憶部２１～２３、切換部２４、カウンタメモリ３２を備えている。しかし、この応答機４１の応答側演算部４２は、後述するように、カウンタメモリ３２のカウンタ情報に基づいて自ら積極的に暗号演算を切り換えるものではなく、後述の指令機４３からの指令信号中に含まれた暗号演算番号に従って暗号演算を切り換える点で、相違する。

【００６７】一方、指令機４３も、前記第２の実施の形態で述べた指令機３３と同様に、ケーシング９、手動スイッチ１０、送信部１１、指令側演算部１２、ＩＤメモリ１３、各暗号演算切換部１５～１７、切換部１８、カウンタ３４を備えている。これに加えて、この指令機４３には、ケーシング９内に着脱可能に装着された電源としての電池（図示せず）が取り出されたか否かを監視し、電池交換を検出したときには、指令側演算部１２に対して暗号演算を強制的に切り換えるための強制切換信号を出力するための強制切換信号生成部（図中では「切換信号生成部」と表記）４４が設けられている点で、相違する。なお、前記「電源」としての電池は、マンガン電池、アルカリ電池、リチウム電池等の種類を問わず、また、その形状もフィルム型、ボタン型、筒型等いずれでもよい。

【００６８】次に、図９及び図１０に基づいて本実施の形態の作用を説明する。まず、図９は、指令機４３側の送信処理を示し、ステップ６１では、強制切換信号生成部４４によって電池の交換（電池がセットされたか否か）を監視しており、電池が新たなにセットされた場合には「ＹＥＳ」と判定して、ステップ６２に移り、このステップ６２では、暗号演算の切換を要求する強制切換信号を発生させる。従って、電池の交換によって、例えば暗号演算の番号を初期値にリセットする等の如く、暗号演算の番号が強制的に切り換えられる。

【００６９】ここで、暗号演算の番号とは、現在使用している暗号演算を特定するための番号であり、例えば、第１の暗号演算記憶部１５には「１」、第２の暗号演算記憶部１６には「２」、第３の暗号演算記憶部１７には「３」の番号が予めセットされており、「暗号化方式を選択するための選択番号」として表現できる。

【００７０】電池を交換したときにカウンタ値の大小に拘わらず暗号演算の番号を切り換えるのは、ユーザーが任意の時点で暗号演算を容易に切り換えることができるようにするためである。これにより、偽指令機が製造されたおそれがある場合等に、ユーザーは、カウンタ情報の累進を待たずに（または時間の経過を待たずに）、簡易に暗号演算を切り換えることができる。そして、前記ステップ６２で暗号演算を強制的に切り換えた後（例えば初期値にリセットした後）、ステップ６３では、この強制切換の情報を記憶しておく。

【００７１】次に、ステップ６４では、手動スイッチ１０が操作されたか否かを判定し、手動スイッチ１０が操作された場合には、ステップ６５で、ＩＤメモリ１３からＩＤコードを読込む。

【００７２】そして、ステップ６６では、カウンタ情報が所定の回数に達したか否かを判定し、所定回数に達していない場合には「ＮＯ」と判定してステップ６７に移り、前回更新された暗号演算を選択する。ここで、前記ステップ６２で暗号演算の切換が行われている場合は、強制切り換えされた暗号演算が選択される。一方、前記ステップ６６で「ＹＥＳ」と判定したときは、カウンタ情報が所定の回数に達した場合のため、ステップ６８では、切換部１８を介して暗号演算を切り換え、ステップ６９では、この新たな暗号演算を更新記憶する。

【００７３】そして、ステップ７０では、前記ステップ６７又はステップ６８で選択された暗号演算に基づいてＩＤコードを暗号化する。次に、ステップ７１では、前記ステップ６３で記憶された切換情報を参照して暗号演算の強制切換が行われた直後であるか否かを判定し、強制切換がされていた場合には、ステップ７２で、応答機４１に強制的な暗号演算の切換が行われたことを報知すべく、強制切換信号（リセット信号）を出力し、ステップ７３で、強制切換情報を消去する。

【００７４】そして、ステップ７４では、例えば下記数４に示す如く、前記ステップ７０で暗号化されたＩＤコードに、カウンタ情報と暗号演算番号（１番の場合を例示）とを付加して送信する。

【００７５】

【数４】C_N，C_{N-1}，…C_1，A_7，A_6，…A_1，１

暗号化ＩＤコードの送信を終了した後、ステップ７５では、カウンタ３４を累進させ、ステップ７６では、電池

が抜かれたか否かを判定する。電池が取り出された場合には、ステップ７６が「ＹＥＳ」と判定し、処理が終了する。

【００７６】次に、図１０は、応答機４１側の受信処理を示し、ステップ８１では、指令機４３からの指令信号を受信したか否かを監視し、受信した場合は「ＹＥＳ」と判定してステップ８２に移る。ここで、指令機４３で電池交換が行われた結果、前記ステップ８１で強制切換信号を受信した場合には、後述するステップ８２及びステップ８３の処理は行われない。

【００７７】次に、ステップ８２では、今回受信した指令信号中のカウンタ情報が前回受信時のカウンタ情報よりも大きいか否かを判定する。このステップ８２で「ＮＯ」と判定した場合は、模造信号か同種の他の指令機４１からの信号を受信した異常な場合のため前記ステップ８１に戻る。一方、前記ステップ８２で「ＹＥＳ」と判定したときは、今回受信時のカウンタ情報が前回受信時よりも大きい正常な場合のため、ステップ８３に移って、指令信号中の暗号演算番号が所定の切換順序に合致しているか否かを判定する。即ち、応答機４１には、過去の受信時の暗号演算番号を記憶した履歴メモリ（図示せず）が設けられており、例えば所定の切換順序が「１→２→３→１…」に設定されている場合、履歴メモリの内容を参照して、今回受信した暗号演算番号が所定の切換順序に一致しているか否かを判定する。但し、カウンタ情報が所定の回数に達するまでは同じ暗号演算番号が引続き使用されるため、切り換えられるまでの間は、「暗号演算番号が変動しているか否か」を判定する。

【００７８】そして、両方の切換順序が一致しないときは、不正な模造信号であるか他の指令信号を受信した異常な場合のため、前記ステップ８３は「ＮＯ」と判定して以後の処理を行わず前記ステップ８１に戻る。一方、切換順序が一致するときは、正常な場合のため、ステップ８４に移って、指令信号中に指定された暗号演算番号と同一の番号の暗号演算記憶部を選択し、この暗号演算に基づいて暗号化されたＩＤコードを復号化する。

【００７９】次に、ステップ８５では、ＩＤメモリ１９からＩＤコードを読込み、ステップ８６では、この応答側のＩＤコードと解読された指令側のＩＤコードとが一致するか否かを判定する。そして、両コードが一致した場合には、前記ステップ８６は「ＹＥＳ」と判定して、ステップ８７に移り、このステップ８７では、ドアロック機構４に制御信号を出力し、次のステップ８８では、カウンタ情報と暗号演算番号とを記憶する。

【００８０】このように構成される本実施の形態でも、前記第２の実施の形態と略同様の効果を得ることができる。これに加えて、本実施例では、以下の効果を奏する。

【００８１】第１に、指令機４３で指定された暗号演算番号に従って、応答機４１は、暗号化されたＩＤコードを解読する構成のため、カウンタ情報が所定の回数以上か否かを判定する処理を不要にでき、制御処理を簡素化することができる。

【００８２】第２に、指令機４３では所定の切換順序に従って暗号演算を切換選択し、応答機４１では、受信信号中の暗号演算番号が所定の切換順序に一致するか否かを判定する構成としたため、指令機４３からの指令信号が正規のものであるか否かを判別することができ、防盗性、信頼性を大幅に向上することができる。

【００８３】第３に、指令機４３で電池交換がされた場合には、暗号演算を強制的に切り換える構成のため、ユーザーは、カウンタ情報の累進を待たずに、所望の任意の時点で暗号演算を容易に手動で切り換えることができる。従って、例えば偽指令機による盗難事故等がユーザーの周囲で発生した場合等には、電池の寿命が到来したか否かに拘わらず、一度電池を取り出して再度セットすることにより、暗号演算を強制的に切り換えて、盗難等を未然に防止することができる。

【００８４】なお、本実施の形態では、電池の交換を検出することにより強制的に暗号演算の切換を行う場合を例示したが、本発明はこれに限らず、例えば指令機４３に別途切換スイッチを設けてもよく、あるいは手動スイッチ１０を所定のパターンでオンオフ操作することにより暗号演算を切り換えるようにしてもよい。但し、電池交換の監視によって暗号演算を切り換える場合は、別途切換スイッチを設ける場合に比較して、構造を簡素化して製造コストを低減できるという有利な効果を奏する。また、電池交換時には、暗号演算番号をリセットして初期値に戻す場合を例に挙げて説明したが、これに限らず、例えば１つ前の暗号演算番号を選択する等の如く、種々の変更も可能である。

【００８５】次に、図１１～図１３に基づいて本発明の第４の実施の形態を説明する。本実施の形態の特徴は、指令機と応答機との間で双方向通信を行うことにより正規の識別コードであるか否かを判定すると共に、経時変化情報として自動車１の状態情報を用いる点にある。

【００８６】即ち、図１１は、本実施の形態に係る遠隔操作装置のブロック図であって、応答機５１は、前記実施の形態で述べたと同様に、受信部６、各暗号演算記憶部２１～２３及び切換部２４を備えている。これに加えて、応答機５１には、後述の指令機５８に応答信号を送信する送信部５２と、第１のＩＤ（以下「ID_1」と略記する）コードを記憶したID_1メモリ５３と、第２のＩＤ（以下「ID_2」と略記する）コードを記憶したID_2メモリ５４と、予め設定された自動車１の状態情報を検出する状態検出部５５と、この状態情報を記憶する状態カウンタ５６とが設けられ、指令機５８との間で双方向通信を行うようになっている。

【００８７】ここで、前記自動車１の状態情報とは、経時変化情報の一例をなすもので、具体的には、例えばイ

グニッションスイッチの操作回数、ドア2の開閉回数、自動車1の走行距離、ウインカーランプの作動回数、ブレーキの作動回数等の如く、経時的に変化する状態情報を意味し、「制御対象に関連して経時的に変化する状態情報」又は「制御対象又は該制御対象に関係付けられた対象に関連して経時的に変化する状態情報」として表現可能なものである。

【0088】一方、指令機58は、ケーシング9、手動スイッチ10、送信部11、各暗号演算記憶部15～17、指令側演算部63及び切換部18を備えている。これに加えて、指令機58には、応答機51からの応答信号を受信するための受信部59と、ID_1コードを記憶したID_1メモリ60と、ID_2コードを記憶したID_2メモリ61と、応答信号中の状態情報を記憶するための状態メモリ62とが設けられている。

【0089】即ち、本実施の形態では、自動車1の状態情報に基づいて暗号演算の切換を決定するため、自動車1側に設けられた応答機51で暗号演算の切換を決定し、この決定を応答信号によって指令機58に報知している。

【0090】次に、図12，図13に基づいて本実施の形態の作用を説明する。まず、図12は指令機58側の処理を示し、ステップ91では、手動スイッチ91が操作されたか否かを判定し、操作された場合は「YES」と判定して、ステップ92でID_1コードを暗号化せずに送信する。そして、このID_1コードが応答機51によって照合確認されると、応答機51からは、自動車1の状態に応じて定まる暗号演算番号が応答信号として送信される。そこで、ステップ93では、この応答機51からの応答信号を受信部59で受信した後、この応答信号で指定された暗号演算番号が所定の切換順序に従っているか否かを判定し、従っているときは、正常な場合なので「YES」と判定してステップ95に移る。

【0091】このステップ95では、切換部18を介して、指定された暗号演算を有する暗号演算記憶部に接続し、この暗号演算を設定する。そして、ステップ96では、設定された暗号演算に基づいてID_2を暗号化し、ステップ97では、この暗号化したID_2を送信部11から送信し、ステップ98では、前記ステップ95で設定された暗号演算を更新して記憶する。

【0092】次に、図13は、応答機51の処理を示し、まず、ステップ100では、状態検出部55を介してイグニッションスイッチの操作回数、走行距離、ドア2の開閉回数等の自動車1の状態情報を検出する。ここで、状態情報は、例示したもののうち、いずれか一つを検出すれば足りるが、複数種類の状態情報を検出し、後述の如く、いずれかの状態情報が所定値に達したときに、暗号演算を切り換える構成としてもよい。

【0093】次に、ステップ101では、前記ステップ100で検出した状態情報が予め設定された所定値に達したか否かを判定する。このステップ101で「NO」と判定したときは、状態情報の値が所定値に達していない場合のため、ステップ102に移り、前回使用した暗号演算を引続き選択する。一方、前記ステップ101で「YES」と判定したときは、暗号演算の切換時期が到来した場合のため、ステップ103に移って状態カウンタ56をリセットし、ステップ104では、所定の切換順序に従って暗号演算を切り換え、ステップ105では、新たな暗号演算を更新記憶する。

【0094】そして、ステップ106では、指令機58からの信号の受信待ちを行い、指令機58からのID_1コード信号を受信した場合には、「YES」と判定してステップ107に移る。ステップ107では、ID_1メモリ53からID_1コードを読込み、ステップ108では、指令機58からのID_1コードと応答機51のID_1コードとが一致するか否かを判定する。このステップ108で「YES」と判定した場合は、両コードが一致する正常な場合のため、ステップ109に移り、前記ステップ102又はステップ105で選択された暗号演算番号を、応答信号として送信部52から指令機58に送信する。

【0095】そして、ステップ110では、前記ステップ109で送信した暗号演算番号に基づいて暗号化されたID_2コードが指令機58から送信されてくるのを待ち、暗号化されたID_2コードを受信した場合には「YES」と判定して、ステップ111に移り、自らが前記ステップ102又はステップ104で指定した暗号演算に基づいて、暗号化されたID_2を復号化する。

【0096】次に、ステップ112では、ID_2メモリ54からID_2コードを読込み、ステップ113では、指令機58からのID_2コードと応答機51が記憶したID_2コードとが一致するか否かを判定する。このステップ113で「YES」と判定したときは、両コードが一致する正常な場合のため、ステップ114に移って、ドアロック機構4に制御信号を出力し、図示せぬ処理ステップで暗号演算番号を記憶する。一方、前記ステップ113で「NO」と判定したときは、両ID2が不一致の場合のため、ステップ100に戻る。

【0097】なお、暗号演算のみで暗号化する場合を例示したが、これに限らず、前記ステップ109で送信する応答信号中に乱数を付加し、この乱数と暗号演算の双方によってID_2コードを暗号化する構成としてもよい。また、応答信号中に状態情報も付加し、指令機58側で状態情報を記憶し、この状態情報に基づいて暗号演算を選択する構成としてもよく、この場合は、暗号演算番号を送信する必要がない。

【0098】このように構成される本実施の形態でも、経時的に変化する自動車1の状態情報に基づいて、暗号演算を切換選択するため、前記各実施の形態と同様の効果を得ることができる上に、以下の効果も発揮する。

【0099】第1に、制御対象としてのドアロック機構4を作動させるのに必要な識別コードをID_1コードとID_2コードとに分割すると共に、指令機58と応答機51との間で双方向通信を行うことにより、先に送信されるID_1コードが一致した場合にのみ、ID_2コードを暗号化して送信する構成としたから、ID_1コードのみならずID_2コードをも入手しない限り、模造信号を生成することができず、防盗性が大幅に向上する。

【0100】第2に、経時変化情報としての自動車1の状態情報に基づいて、暗号演算の切換時期を決定する構成のため、前記第2の実施の形態で述べたカウンタ情報を利用する場合と同様に、暗号演算の切換時期を変則的にして、防盗性、信頼性を向上することができる。さらに、この状態情報は、自動車1側でのみ生成される特質を有し、かつ、この状態情報に基づいて専ら応答機51側で暗号演算を指定する構成だから、模造信号を作成するために自動車1内に固定された応答機51を調査する必要が生じ、防盗性等を一層向上することができる。

【0101】なお、前記各実施の形態では、自動車用ドアロックシステムに適用した場合を例示し、制御対象としてドアロック機構4を挙げたが、これに限らず、例えば家庭電気製品、工作機械等の他の防盗性を要するものにも適用できる。

【0102】また、暗号演算の切換順序を監視するステップは、第1の実施の形態、第2の実施の形態にも適用することができる。

【0103】同様に、電池交換を監視して強制的に暗号演算を切り換える構成は、他の実施の形態にも容易に適用することができる。

【0104】さらに、各処理のフローチャートは、その要部を簡潔に示しているため、例えば、識別コードが一致しない等のエラーが所定回数以上続いたときには、受信待機状態を解除して、一定時間の間の受信を拒否したり、エラーメッセージ又は警報を発したりする等の如く、当業者であれば、種々の改良、追加、変更が可能である。

【0105】また、第4の実施の形態では、識別コードを2分割する場合を例に挙げて説明したが、これに限らず、例えば3分割、4分割等して、各識別コードが一致する場合にのみ制御信号を出力する構成も当業者であれば容易に想到できる。

【0106】なお、前記各実施の形態では、ステップ1，12，32，42，75，82，100が「経時変化情報検出手段」の具体例である。また、ステップ6，15，36，45，68，95，104が「選択手段」の具体例である。さらに、ステップ8，38，70，96が「暗号化信号生成手段」の具体例である。また、ステップ17，47，84，111が「復号化手段」の具体例である。さらに、ステップ20，50，87，114が「制御信号出力手段」の具体例、ステップ83，94が「切換順序監視手段」の具体例をそれぞれ示す。また、前記ステップ62が「強制切換信号生成手段」の具体例である。

【0107】

【発明の効果】以上詳述した通り、本発明の請求項1、請求項2、請求項6及び請求項8に係る遠隔操作装置又は遠隔操作方法によれば、時間の経過と共に変化する経時変化情報によって暗号化方式が切り換えられるため、ある時点で指令機が模造された場合でも、経時変化情報に基づいて他の暗号化方式に切り換えられた時点で、この偽指令機を無力化することができるため、所定サイクル毎に、遠隔操作装置の信頼性、防盗性を回復し、維持できる。

【0108】また、請求項3に係るものでは、制御信号出力手段を駆動するのに必要な識別コードを第1の識別コードと第2の識別コードとに分割し、かつ、第2の識別コードは経時変化情報に基づいて切り換えられる暗号化方式によって暗号化するため、より一層防盗性、信頼性を高めることができる。

【0109】さらに、請求項4に係るものでは、万が一、正規の指令機が記憶する複数種類の暗号化方式を全て複製した模造指令機が製造された場合であっても、その切換順序が異なれば、応答機によって制御対象を動作させることができないため、より一層防盗性、信頼性を高めることができる。

【0110】また、請求項5に係るものでは、実際に経時変化情報を検出するのは指令機又は応答機の経時変化情報検出手段のうちいずれか一方のみで足り、他方は、その検出された値を自己の検出値として間接的に検出するため、全体構造を簡素化しつつ、指令機と応答機との間で経時変化情報にずれが生じるのを確実に防止することができる。

【0111】さらに、請求項7に係るものでは、強制切換信号生成手段によって強制的に暗号演算の切換を可能としたため、ユーザーが任意の時点で容易に暗号演算を切り換えることができ、より一層防盗性を向上することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る遠隔操作装置を適用した自動車用ドアロック装置の全体構成を示す構成説明図である。

【図2】指令機及び応答機の具体的なブロック構成図である。

【図3】指令機による送信処理を示すフローチャートである。

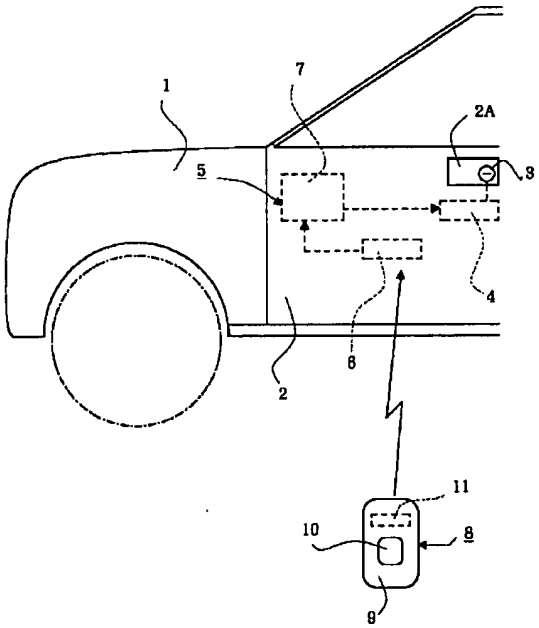
【図4】応答機による受信処理を示すフローチャートである。

【図5】本発明の第2の実施の形態に係る遠隔操作装置のブロック図である。

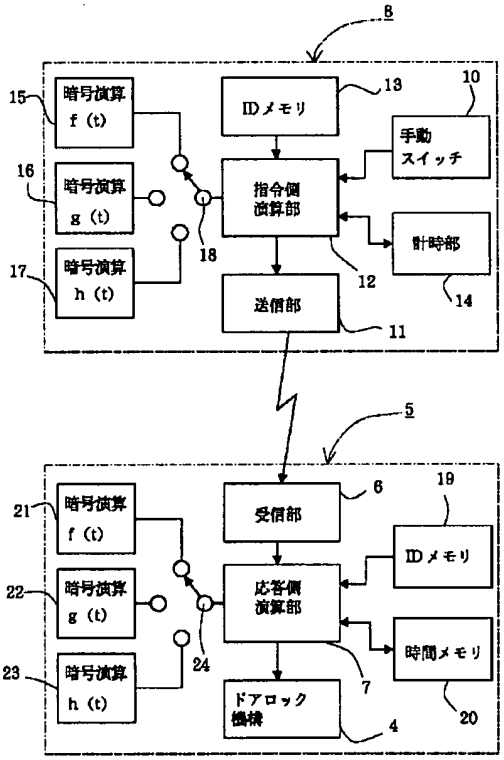
【図6】指令機による送信処理を示すフローチャートで

ある。
【図７】応答機による受信処理を示すフローチャートである。
【図８】本発明の第３の実施の形態に係る遠隔操作装置のブロック図である。
【図９】指令機による送信処理を示すフローチャートである。
【図１０】応答機による受信処理を示すフローチャートである。
【図１１】本発明の第４の実施の形態に係る遠隔操作装置のブロック図である。
【図１２】指令機による処理を示すフローチャートである。
【図１３】応答機による処理を示すフローチャートである。
【符号の説明】
１…自動車
２…ドア
４…ドアロック機構（制御対象）
５，３１，４１，５１…応答機
８，３３，４３，５８…指令機
ＩＤ，ID_1，ID_2…識別コード

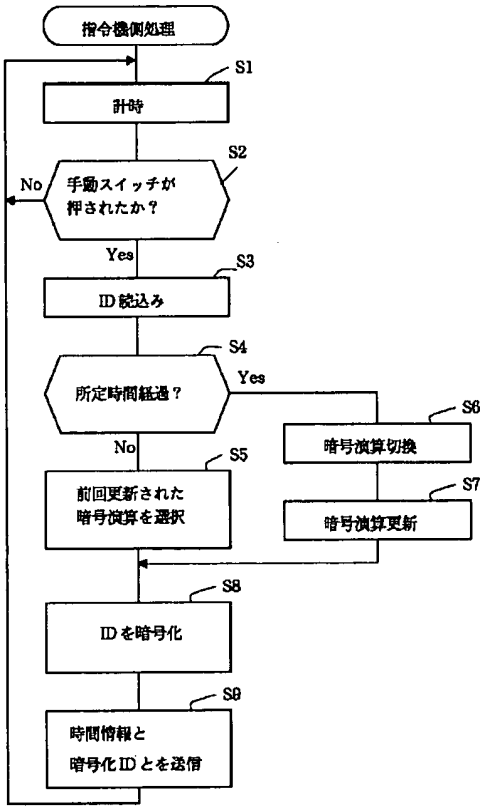
【図１】



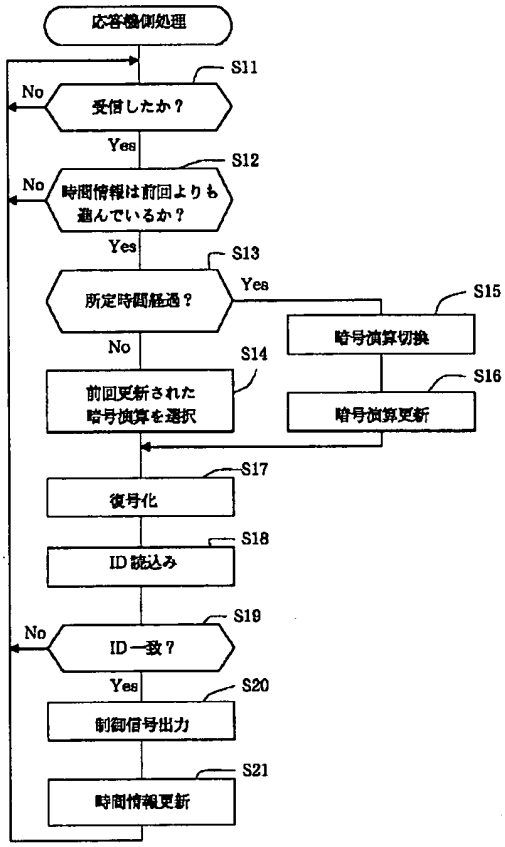
【図２】



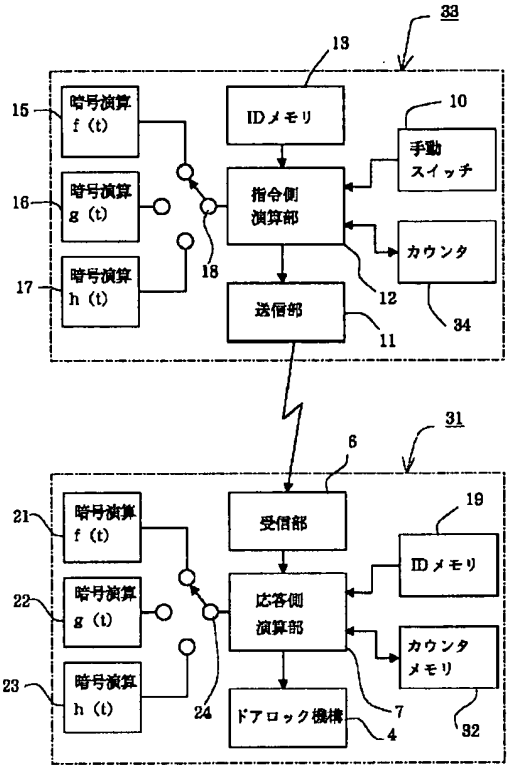
【図3】


指令機側処理
S1
計時
S2
No
手動スイッチが
押されたか？
Yes
S3
ID読込み
S4
所定時間経過？
Yes
S6
暗号演算切換
No
S5
前回更新された
暗号演算を選択
S7
暗号演算更新
S8
IDを暗号化
S9
時間情報と
暗号化IDとを送信

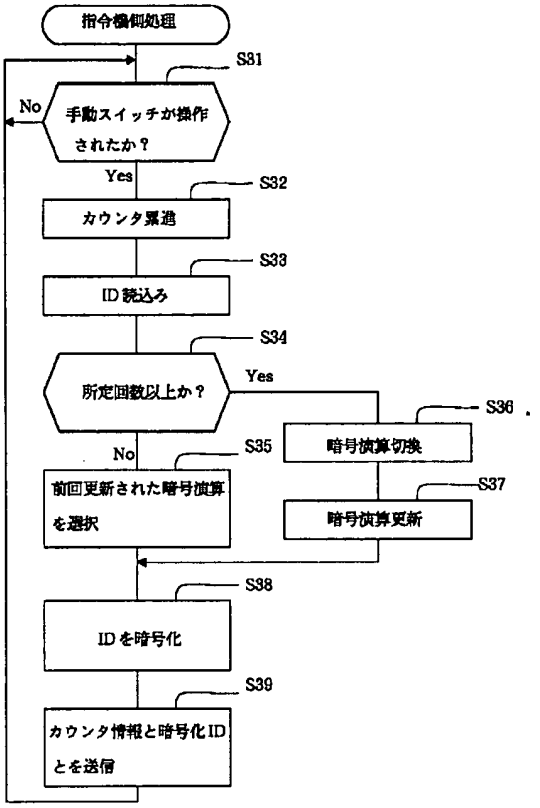
【図4】


応答機側処理
S11
No
受信したか？
Yes
S12
No
時間情報は前回よりも
遅んでいるか？
Yes
S13
所定時間経過？
Yes
S15
暗号演算切換
No
S14
前回更新された
暗号演算を選択
S16
暗号演算更新
S17
復号化
S18
ID読込み
S19
No
ID一致？
Yes
S20
制御信号出力
S21
時間情報更新

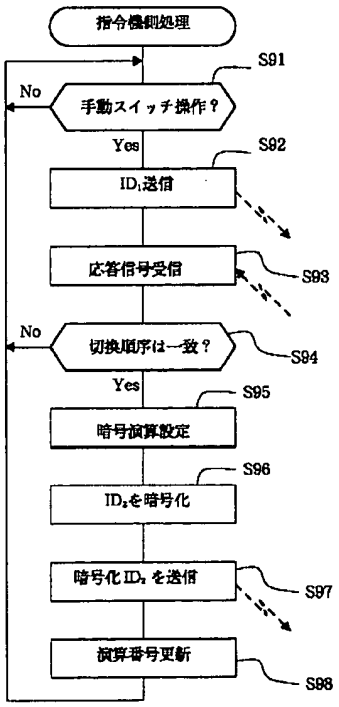
【図5】


33
13
15
暗号演算
f (t)
IDメモリ
10
手動
スイッチ
16
暗号演算
g (t)
指令側
演算部
カウンタ
17
暗号演算
h (t)
18
送信部
12
34
11
31
6
21
暗号演算
f (t)
受信部
19
IDメモリ
22
暗号演算
g (t)
応答側
演算部
カウンタ
メモリ
23
暗号演算
h (t)
24
ドアロック機構
7
4
32

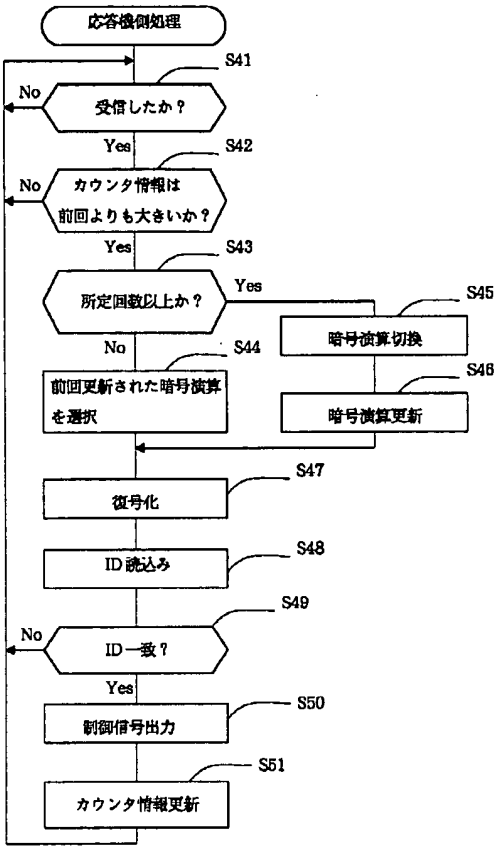
【図6】


指令機側処理
S31
No
手動スイッチが操作
されたか？
Yes
S32
カウンタ累進
S33
ID読込み
S34
所定回数以上か？
Yes
S36
暗号演算切換
No
S35
前回更新された暗号演算
を選択
S37
暗号演算更新
S38
IDを暗号化
S39
カウンタ情報と暗号化ID
とを送信

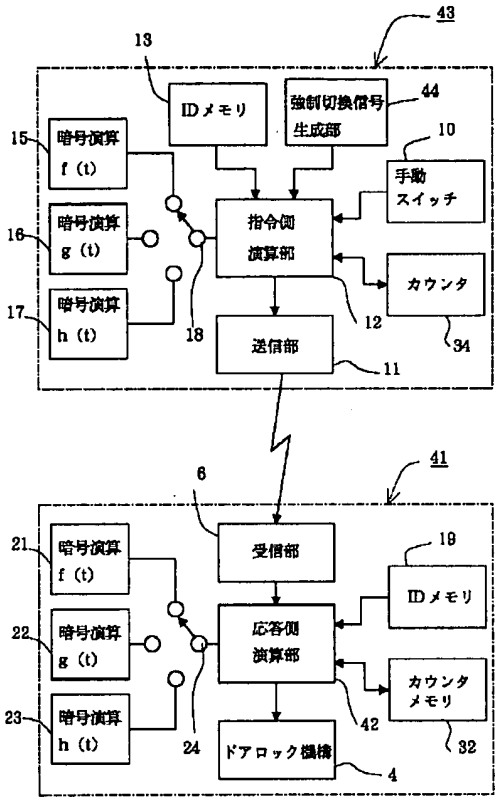
【図12】


指令機側処理
S91
No
手動スイッチ操作？
Yes
S92
ID1送信
応答信号受信
S93
No
切換順序は一致？
S94
Yes
S95
暗号演算設定
S96
ID2を暗号化
暗号化ID2を送信
S97
演算番号更新
S98

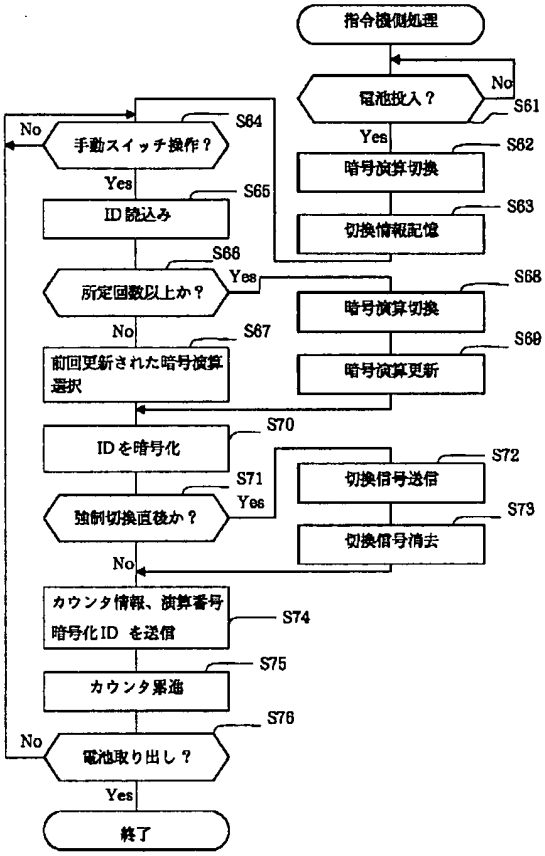
【図7】


応答機側処理
S41
No
受信したか？
Yes
S42
No
カウンタ情報は
前回よりも大きいか？
Yes
S43
所定回数以上か？
Yes
S45
暗号演算切換
No
S44
前回更新された暗号演算
を選択
S46
暗号演算更新
S47
復号化
S48
ID読込み
S49
No
ID一致？
Yes
S50
制御信号出力
S51
カウンタ情報更新

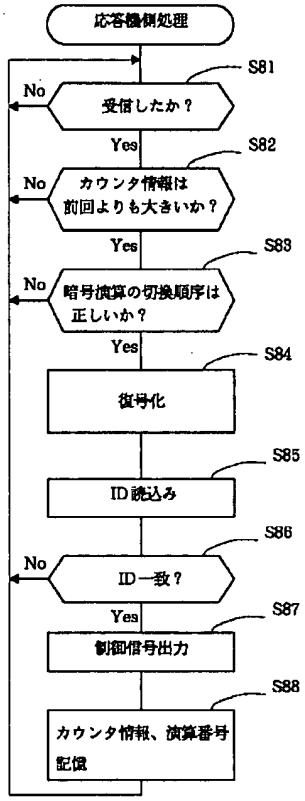
【図8】


43
13
IDメモリ
強制切換信号
生成部
44
10
15
暗号演算
f (t)
手動
スイッチ
16
暗号演算
g (t)
指令側
演算部
カウンタ
17
暗号演算
h (t)
18
12
送信部
34
11
41
6
受信部
21
暗号演算
f (t)
19
IDメモリ
22
暗号演算
g (t)
応答側
演算部
カウンタ
メモリ
23
暗号演算
h (t)
24
42
ドアロック機構
32
4

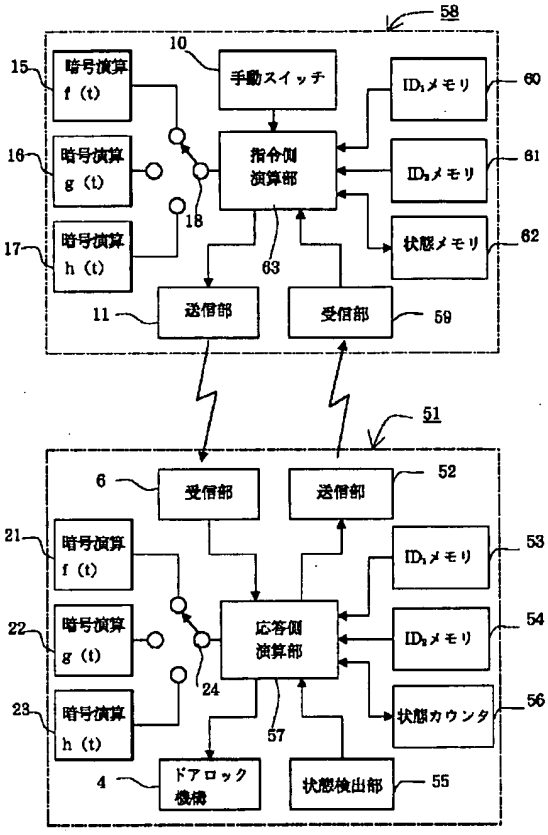
【図9】


指令機側処理
電池投入？
No
S61
Yes
暗号演算切換
S62
切換情報記憶
S63
S64
No
手動スイッチ操作？
Yes
S65
ID読込み
S66
所定回数以上か？
Yes
S68
暗号演算切換
No
S67
前回更新された暗号演算選択
S69
暗号演算更新
S70
IDを暗号化
S71
Yes
強制切換直後か？
S72
切換信号送信
S73
切換信号消去
No
カウンタ情報、演算番号
暗号化ID を送信
S74
S75
カウンタ累進
S76
No
電池取り出し？
Yes
終了

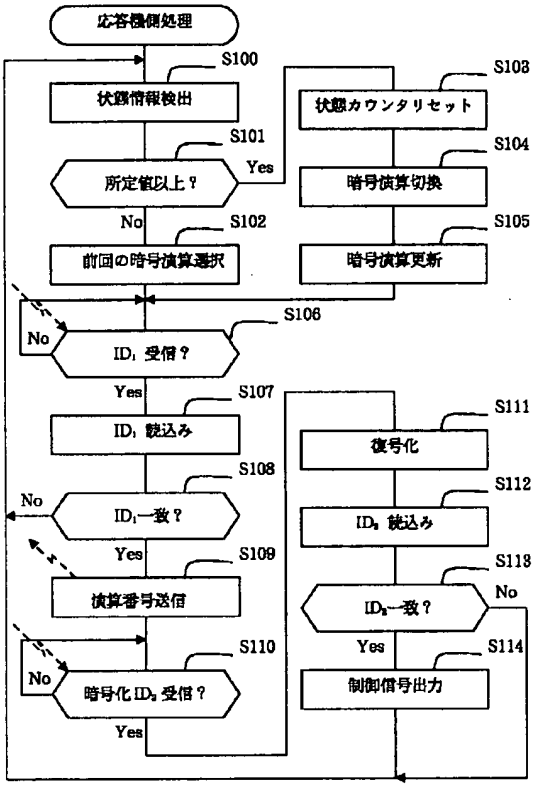
【図10】


応答機側処理
S81
No
受信したか？
Yes
S82
No
カウンタ情報は
前回よりも大きいか？
Yes
S83
No
暗号演算の切換順序は
正しいか？
Yes
S84
復号化
S85
ID読込み
S86
No
ID一致？
Yes
S87
制御信号出力
S88
カウンタ情報、演算番号
記憶

【図11】


58
10
15
暗号演算 f (t)
手動スイッチ
ID1メモリ
60
16
暗号演算 g (t)
指令側 演算部
ID2メモリ
61
18
17
暗号演算 h (t)
状態メモリ
62
63
11
送信部
受信部
59
51
6
受信部
送信部
52
21
暗号演算 f (t)
ID1メモリ
53
22
暗号演算 g (t)
応答側 演算部
ID2メモリ
54
24
23
暗号演算 h (t)
状態カウンタ
56
57
4
ドアロック 機構
状態検出部
55

【図13】


応答機側処理
S100
状態情報検出
S101
所定値以上？
Yes
No
S102
前回の暗号演算選択
S103
状態カウンタリセット
S104
暗号演算切換
S105
暗号演算更新
No
S106
ID1 受信？
Yes
S107
ID1 読込み
S108
No
ID1一致？
Yes
S109
演算番号送信
No
S110
暗号化ID2 受信？
Yes
S111
復号化
S112
ID2 読込み
S113
No
ID2一致？
Yes
S114
制御信号出力